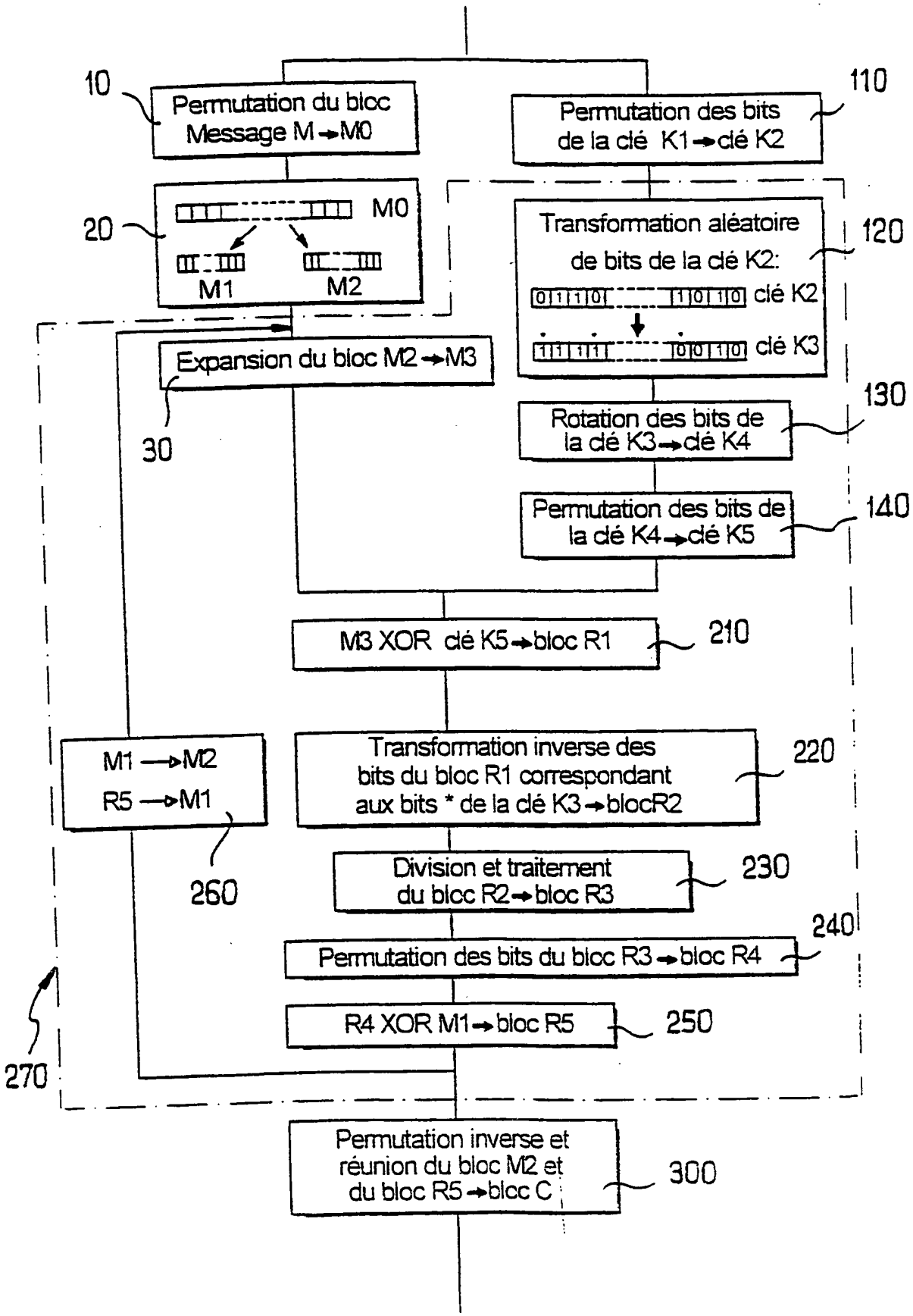
10
Permutation du bloc Message M→M0
110
Permutation des bits de la clé K1→clé K2
20
M0
M1
M2
Transformation aléatoire de bits de la clé K2:
120
clé K2
clé K3
Expansion du bloc M2→M3
30
130
Rotation des bits de la clé K3→clé K4
140
Permutation des bits de la clé K4→clé K5
M3 XOR clé K5→bloc R1
210
M1 →M2
R5 →M1
260
Transformation inverse des bits du bloc R1 correspondant aux bits * de la clé K3→blocR2
220
Division et traitement du bloc R2→bloc R3
230
240
Permutation des bits du bloc R3→bloc R4
R4 XOR M1→bloc R5
250
270
Permutation inverse et réunion du bloc M2 et du bloc R5→bloc C
300